REMARKS/ARGUMENTS

Reconsideration of the application is respectfully requested. Claims 1-27 are pending in the present invention. No new matter has been added to the application in this response.

1. Rejection of Claims 1-5, 7-10, 22-24 and 26-27 under 35 USC § 102(e).

Claims 1-5, 7-10, 22-24 and 26-27 were rejected under Section 102 as being anticipated by Linnakangas. This § 102 rejection is respectfully traversed.

In summary, one problem with standard IPSsec is that the end points of the IPSec tunnel mode SA (security association) are fixed. There is no feature in conventional systems for changing any of the parameters of an SA other than by establishing a new SA that replaces the previous SA. More particularly, since mobile terminals move and thus change their network points frequently and since IPSec connections are bound to fixed addresses, the mobile terminals must establish new IPSec connections from each point of attachment. This requires the exchange of keys etc. which is a cumbersome process that uses computation time. The method of the present invention provides a solution to this problem. One unique feature of the present invention is that the intermediate

computer modifies the addresses and SPI values of the same pre-existing secure connection i.e. without requiring the setting up of a new secure connection. In this way, a secure message sent from the first computer to the intermediate computer may be modified so that it can be forwarded from the intermediate computer to the second computer in the same secure connection without requiring the cumbersome exchange of additional keys of a new secure connection and without involving the second computer.

a. The Requisite Steps of Independent Claim 1 Are Neither Taught Nor Suggested in the Cited Art.

Claim 1 has been amended to clarify that the secure connection extends between the source address of the first computer as the first end point of the secure connection and the destination address of the second computer as the second end point of the secure connection. The claim has also been modified to clarify that the intermediate computer substitutes the first destination address with the second destination address and substitutes the first unique identity with a second unique identity of the secure connection without establishing a new secure connection and without involving the second computer. No new matter has been added to the amended claim 1 or any other claim. For example, support may be found on pages 12, 14, 17, 19-21 of the original patent

specification WO 03/063443. It is submitted that such steps are not taught or suggested in the cited references.

On page 3, paragraph 7, the Examiner refers to paragraph 4 and paragraph 24, lines 4-8 of Linnakangas as teaching the step of secure forwarding of a message from a first computer (local host 5) to a second computer via an intermediate computer in a telecommunication network. It should be noted that claim 1 has been amended to clarify that the end points of the secure connection extend between the first computer and the second computer. Claim 1 has also been amended to require that the intermediate computer substitutes the first unique identity with a second unique identity of the same secure connection without establishing a new secure connection and without involving the second computer.

Applicants submit that Linnakangas completely fails to teach these additional steps and limitations. Linnakangas' IPSec is only between the remote host 4 and the router 2. There is no secure connection between the local host 5 and the router 2. In contrast, the router 2 decrypts, reads and unwraps the secure message from the remote host 4 to be able to determine that the message is to be forwarded to the local host 5. This forwarding is done without implementing IPSec. The Examiner is respectfully requested to show where Linnakangas teaches that the secure connection extends between the local host 5

and the router 2 also. On page 2, the Examiner writes that "a virtual private network is established to provide secure communication between host 4 and host 5, via router 2 (See par. 24, 4-8). Thus a secure communication is provided between host 5 and router 2."

Linnakangas clearly fails to teach or suggest a secure connection that extends between the source address of the host 4 as a first end point and the destination address of the host 5 as the second end point of the secure connection. Additionally, Linnakangas fails to teach the step of the router 2 substituting the first unique identity with the second unique identity of the secure connection without establishing a new secure connection and without involving the second computer; and the router 2 forwarding the secure message to the second computer in the same secure connection.

In paragraph 24, lines 4-8, Linnakangas explains that "[b]y using IPSec to control communication between the router 2 and the remote hosts 4 (and hence between remote hosts 4 and local hosts 5), a Virtual Private Network (VPN) may be established" (emphasis added). It is respectfully submitted that this is different from a secure connection that has end points extending between the host 4 and the host 5. Additionally, "controlling" communication across the route from remote host 4 via router 2 all the way to host 5 does not mean here that

there is a secure connection also between router 2 and host 5. Linnakangas merely mentions controlling the communication, not securing. In other words, the IPSec, defined in the foregoing sentence in Linnakangas as being between the host 4 and the router 2, controls what traffic goes therebetween. The traffic from the host 4 to host 5 goes via this IPSec connection between the host 4 and router 2. It should be noted that the virtual private network in Linnakangas is note secured but merely controlled. There is not really as much need for a secure connection between the router 2 and the host 5 since the connection is within the same LAN. Wikipedia states that a virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger networks (such as the Internet), as opposed to running across a single private network. The Link Layer protocols of the virtual network are said to be tunneled through the transport network. One common application is to secure communications through the public Internet, but a VPN does not need to have explicit security features such as authentication or content encryption and is quite different from a secure connection such as a security association.

Applicants also would like to draw the Examiner's attention to the fact that, in the cited Linnakangas paragraph, the establishment of the secure connection between remote host 4

and router 2 is quite well described, including the exchange of keys etc. However, there is nowhere described any security connection formed between router 2 and host 5, because there is no security connection between router 2 and host 5. Paragraph 24 of Linnakangas merely teaches the remote host 4 negotiating secure associations with the router 2 (lines 9-10 of paragraph 24). There is nothing about forming a secure message in the local host 5 or negotiating secure associations with the local host 5. Even if the communication between the router 2 and the host 5 may be considered quite safe and secure, Linnakangas still completely fails to teach or suggest establishing a secure connection that extends between a source address of the host 4 as a first end point and the destination address of the host 5 as the second end point of the same secure connection.

Applicants cannot see that Linnakangas teaches the required steps of establishing a secure connection between the first computer and the second computer wherein the secure connection extends between a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection.

It is submitted that Linnakangas also fails to teach or suggest the step of the intermediate computer, while being in a secure connection between the first computer and the second

computer as required in the first paragraph of the amended claim 1, the intermediate computer substituting the first unique identity with a second unique identity of the same secure connection without establishing a new secure connection and without involving the second computer, and the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the same secure connection.

It is submitted that Linnakangas completely fails to teach or suggest the above-outlined steps. Therefore, the rejection of claim 1 under § 102 is improper, and should be removed.

b. Dependent Claims 2-5 and 7-10

Claims 2-5, 7-10 are submitted to be allowable because the claims depend either directly or indirectly upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in the cited references.

2. The Requisite Limitations of Independent Claim 22 Are Neither Taught Nor Suggested in the Cited Art.

As mentioned above, Linnakangas merely shows a secure connection between the remote host 4 and the router 2. Applicants fails to see where Linnakangas teaches a secure

connection that has a source address of the host 4 (the first computer) as a first end point and a destination address of the local host 5 (the second computer) as a second end point. In contrast, the secure connection of Linnakangas merely extends between the host 4 and the router 2. Additionally, Linnakangas fails to teach or suggest means for forwarding the secure message received from the first computer to the second computer in the secure connection. In contrast, Linnakangas merely describes a router 2 that forwards a message in a VPN and an IPSec with end points at the host 4 and the router 2 (but not at the host 5).

It is submitted that Linnakangas fails to teach or suggest all the limitations of the amended claim 22. Therefore, the anticipation rejection of claim 22 under § 102 is improper, and should be removed.

a. Dependent claims 23-24 and 26

Claims 23-24 and 26 are submitted to be allowable because the claims depend either directly or indirectly upon the allowable base claim 22 and because each claim includes limitations that are not taught or suggested in the cited references.

3. The Requisite Limitations of Independent Claim 27 Are Neither Taught Nor Suggested in the Cited Art.

Similar to claim 22, the amended claim 27 requires a secure connection that has a source address of the first computer as a first end point and a destination address of the second computer as a second end point. The amended claim 27 also requires that the intermediate computer has means for forwarding the secure messages received from the first computer to the second computer in the secure connection. The amended claim 27 is submitted to be allowable for reasons similar to the reasons put forth for the allowability of the amended claim 1 and claim 22.

It is submitted that Linnakangas fails to teach or suggest all the limitations of the amended claim 27. Therefore, the rejection of claim 27 under § 102 is improper, and should be removed.

4. Rejection of Claims 6, 11-14 and 20-21 under 35 USC § 103(a).

Claims 6, 11-14 and 20-21 were rejected under Section 103 as being obvious over Linnakangas, as applied to claim 1 above, in view of Applicant's Admitted Prior Art (AAPA). This § 103 rejection is respectfully traversed in part and overcome in part as follows:

a. The Requisite Steps of Claims 6, 11-14 and 20-21 Are Neither Taught Nor Suggested in the Cited Art.

Claims 6, 11-14 and 20-21 are submitted to be allowable because the claims depend either directly or indirectly upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in the cited references.

The § 103 rejection is therefore improper and should be withdrawn.

b. Prima Facie Support for Combination Under § 103 Not Provided

Even assuming *arguendo* that the requisite method steps of claims 6, 11-14 and 20-21 are shown by the combination of Linnakangas and AAPA, *prima facie* support for combining the references, according to the requirements as set forth in M.P.E.P. § 2142 has not been provided in the present Office Action.

As provided in M.P.E.P. § 2142, the Supreme Court in *KSR International v. Teleflex Inc.*, 82 USPQ2d 1385, 1396 (2007) specified that the analysis supporting a rejection under 35 U.S.C. § 103 should be made explicit. "[R]ejections on

obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn,* 441 F.3dd 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). Furthermore, the Examiner must make "explicit" this rationale of "the apparent reason to combine the known elements in the fashion claimed," including a detailed explanation of "the effects of demands known to the design community or present in the marketplace" and "the background knowledge possessed by a person having ordinary skill in the art" (KSR, page 14).

The only rationale provided in support of the 103(a) rejection of claim 6 is at the bottom of page 7 of the Office action, which merely asserts it would have been obvious to modify the teaching method of Linnakangas with AAPA because it "would have added flexibility by allowing different networks to connect to the system"(emphasis added). It seems that the Examiner has completely ignored the arguments put forth in the previous response regarding the Examiner's failure to establish a *prima facie* case of obviousness. Applicants request the Examiner to consider all of the arguments of this response instead of simply copying text from the previous Office action.

The Examiner has again merely provided one benefit, or

advantage of the modification ass the only rationale provided in the Office Action in support of the instant rejection.

However, merely stating that a benefit of the modification exists, as done above, does not provide the "articulated reasoning with some rationale underpinning to support the legal conclusion of obviousness, required under *KSR*. By definition, every patentable invention must be "beneficial" - and *arguendo* every invention contemplates at least some new benefit(s) in arriving at the invention - certainly this does not render the benefit obvious or expected. Because every modification or element has a corresponding use or benefit, the above reasoning could be applied to any improvement. It appears therefore that "hindsight construction" may have perhaps played a role in arriving at the present ground for rejection in the Office action - which though difficult perhaps to avoid in many cases, is nonetheless impermissible in making a *prima facie* showing of obviousness.

According to M.P.E.P. 2142, "the examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness." Because a *prima facie* conclusion of obviousness has not been provided in the present Office Action, Applicants respectfully request reconsideration and

withdrawal of this ground for rejection as to claim 6.

Similarly, no articulated reasoning is provided for the rejections of claims 11-14 and 20-21. On page 8, lines 5-7, the Examiner merely states it would have been obvious because it "would have broadened the appeal and applicability of the system by allowing mobile units to connect to the network" (emphasis added). On page 9, lines 1-2 and 8-9 of the Office action it is stated that the combination would have been obvious because it "would have added improved security to the system" (emphasis added). It is submitted that none of the above stated general benefits provides the required articulated reasoning to show *prima facie* conclusion of obviousness.

The rejections of claims 6, 11-14 and 20-21 under Section 103 are therefore improper and should be removed.

5. Rejection of Claims 15-19 and 25 under 35 USC § 103(a).

Claims 15-19 and 25 were rejected under Section 103 as being obvious over Linnakangas in view of Sandhu. This rejection is respectfully traversed.

a. The Requisite Steps of Claims 15-19 and 25 Are Neither Taught Nor Suggested in the Cited Art.

Claims 15-19 and 25 are submitted to be allowable because the claims depend either directly or indirectly upon the allowable base claims 1 and 22, respectively, and because each claim includes limitations that are not taught or suggested in the cited references.

The § 103 rejection is therefore improper and should be withdrawn.

b. Prima Facie Support for Combination Under § 103 Not Provided

These rejections also lack the required articulated reasoning to establish *prima facie* conclusion of obviousness. The only reasons for obviousness are stated on page 9, last line ("would have added another layer of security within the secure connection" (emphasis added)) and page 10, line 15 ("would have increased the number of security features available in the system" (emphasis added)) are again submitted to be mere general benefits that do not provide the required articulated reasoning to meet the burden of establishing a *prima facie* conclusion of obviousness. Page 12, lines 2-3, of the Office action states that the proposed combination is obvious because it "would have provided increased security and insured that messages where transmitted to the correct destination" (emphasis added). It is assumed that the Examiner meant that

messages "were" transmitted to the correct destination. Again the above statements fail to establish the prima facie case of obviousness since they merely mention benefits and advantages of the proposed combination, as explained above.

The rejections of claims 15-19 and 25 under Section 103 are therefore improper and should be removed.

6. Conclusion

Based on the foregoing, Applicants respectfully request that the various grounds for rejection in the Office Action be reconsidered and withdrawn with respect to the previously amended form of the claims, and that a Notice of Allowance be issued for the present application to pass to issuance.

In the event any further matters remain at issue with respect to the present application, Applicants respectfully request that the Examiner please contact the undersigned below at the telephone number indicated in order to discuss such matter prior to the next action on the merits of this application.

The application is submitted to be in condition for allowance, and such action is respectfully requested.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/
Rolf Fasth
Registration No. 36,999

ATTORNEY DOCKET NO. 290.1078USN

FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301

Telephone: (910) 687-0001
Facsimile: (910) 295-2152